# National Cybersecurity Center of Excellence (NCCoE)

## Consumer/Retail Sector Webinar

- Multifactor Authentication for e-Commerce
- Securing Non-Credit Card, Sensitive Consumer Data

Bill Newhouse & Sarah Weeks

June 21, 2016

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

# AGENDA

| | | |
|---|---|---|
| **12:00 PM** | Introduction to NCCoE | 5 min |
| **12:05 PM** | Background of Retail projects | 5 min |
| **12:10 PM** | Overview of MFA project | 5 min |
| **12:15 PM** | Overview of Data project | 5 min |
| **12:20 PM** | Deep dive into MFA project architecture and technical implementation | 17 min |
| **12:37 PM** | Deep dive into Data project architecture and technical implementation | 17 min |
| **12:54 PM** | Closing remarks/Next steps | 6 min |

# ENGAGEMENT & BUSINESS MODEL

| DEFINE + ARTICULATE<br>Describe the business problem | ORGANIZE + ENGAGE<br>Partner with innovators | IMPLEMENT + TEST<br>Build a reference design | TRANSFER + LEARN<br>Guide stronger practices |
|---|---|---|---|
| ACTION | ACTION | ACTION | ACTION |
| Identify and describe business problem | Publish project description and solicit responses | Build reference design | Collect documents |
| Conduct market research | Select partners and collaborators | Test reference design | Tech transfer |
| Vet project descriptions | Sign CRADA | Identify gaps | Document lessons learned |
| OUTCOME | OUTCOME | OUTCOME | OUTCOME |
| Define business problems and project descriptions, refine into specific use case | Collaborate with partners from industry, government, academia and the IT community on reference design | Practical, usable, repeatable reference design that addresses the business problem | Set of all material necessary to implement and easily adopt the reference design |

# CONSUMER-FACING/RETAIL SECTOR WORK BACKGROUND

## Executive Technical Workshop on Improving Cybersecurity and Consumer Privacy (Feb 2015)

- Held in conjunction with the White House Summit on Cybersecurity and Consumer Protection
- Nearly 200 individuals participated in workshop
- Retail & point-of-sale cybersecurity concerns identified were highlighted in NISTIR 8050 (Apr 2015)

## (Panel Discussion) Cybersecurity in Retail: Trends and Challenges with Point-of-Sale and Payment Technologies (Nov 2015)

- Panelists from National Retail Federation, Retail Industry Leaders Association, PCI Security Standards Council, FS-ISAC
- Broader discussion on cybersecurity challenges in this space

## National Retail Federation BIG Show Briefings (Jan 2016)

- CIO Council, IT Security Council, ARTS (NRF’s Retail Technology Standards Division) conversations
- Over 100 participants in various conversations
- Outcome: specific technical challenges around authentication and securing data in a retail environment
  - Multifactor authentication for online/e-commerce transactions
  - Securing non-credit card, sensitive consumer data

# CONSUMER-FACING/RETAIL SECTOR WORK BACKGROUND

## Workshop - Protecting Consumer Data: Securing Payment and Transaction Information

- Held at University of Alabama at Birmingham (NCCoE) Academic Affiliate Council member), March 2016
- More than 160 individuals participated in person or via online webcast
- Two panels composed of retailers, standards organizations, security or payment processing technology vendors, and information sharing and analysis centers, discussed the proposed projects in the Retail sector space:
  - Multifactor Authentication for e-Commerce
  - Securing Non-Credit Card Consumer Data

## Working Session - Working Together: Addressing Retail Cybersecurity With Standards and Best Practices

- At the Retail Cyber Intelligence Sharing Center (R-CISC) Summit, April 2016
- Discussion of proposed projects in the Retail sector space with retailers and partners
- Comment period closed, June 3, 2016

## Draft Special Publication 800-63-3: Digital Authentication Guideline

- Public Preview on https://pages.nist.gov/800-63-3/

- **In our project description we propose that a multifactor authentication solution for e-commerce transactions includes the components listed below.**
  - Online/e-commerce shopping cart and payment system (in-house or outsourced)
  - Multifactor authentication mechanisms
  - Risk calculation platform/engine
  - Web analytics engine
  - Logging of risk calculation and web analytics data
  - Data storage for risk calculation and web analytics data
- **What else would be realistic to include in an architecture representative of online retail webshops/shopping portals?**
- **When and where are third party products or services leveraged in a typical online retail ecosystem? What interfaces between retailer owned pieces and third-party pieces should we be aware of and include in the project?**

- **We propose that MFA should be part of a system of multiple solutions necessary to successfully reduce e-Commerce fraud. What other fraud solutions exist, and how would MFA fit into existing anti-fraud paradigms in online retail?**
- **It is extremely important to retail business that the user experience must not be impeded by additional security mechanisms. With that in mind, where in the lifecycle of an e-commerce transaction would it be reasonable to include an MFA mechanism?**
  - **And which types/forms of MFA mechanisms would be realistic to implement?**
- **Are there significant differences in multifactor authentication for e-commerce transaction architectures depending on the incorporation of Cloud or On-Premise technologies?**
- **We are aware of ARTS, NIST, and ISO standards that may apply and or concern retailers in implementing their systems and system security. Are there other standards we should be aware of and apply to our projects?**

- **In our project description we propose that a securing non-credit card, sensitive consumer data architecture includes the components listed below.**
  - Online retail website or simulated customer service portal with loyalty program registration
  - Tokenization mechanism
  - Secure data store for tokens
  - Secure data vault for actual data
  - Data masking mechanism
  - Attribute Based Access Control (ABAC) platform
    - Policies
    - Decision making
    - Decision enforcement
- **What else would be realistic to include in an architecture representative of the backend or internal retail system?**

# DISCUSSION POINTS AND QUESTIONS: SECURING NON-CREDIT CARD, SENSISTIVE CONSUMER DATA

- **Besides “cardholder data” as defined by the PCI DSS, what types of data do retailers and their partners/third party service providers collect?**
- **What mechanisms if any are already in place for protecting non-cardholder data?**
  - **P2P Encryption?**
- **In addition to what is already in place (as discussed in the previous question), are data tokenization, data masking, and fine grained access control realistic to implement within a retail organization and among its partners?**
  - **Which internal and external users and partners need access to raw data?**
  - **Do retailers or partners, or both, store non-cardholder consumer data?**
  - **Where is non-cardholder most vulnerable in internal/backend retailer systems?**

# DISCUSSION POINTS AND QUESTIONS: SECURING NON-CREDIT CARD, SENSISTIVE CONSUMER DATA

- **Are there significant differences in securing data depending on the incorporation of Cloud or On-Premise technologies?**
- **We are aware of ARTS, PCI, NIST, and ISO standards that may apply and or concern retailers in implementing their systems and system security. Are there other standards we should be aware of and apply to our projects?**

# BACKUPS

## BACKUPS

# MULTIFACTOR AUTHENTICATION FOR ONLINE TRANSACTIONS

- Retailers note that EMV implementation will shift fraud to card-not-present (CNP) transactions
- Retailers have noted that secure card-not-present (CNP) transactions will become more critical but hard for them to solve challenges due to competing business priorities
- Reference design to take into account need for frictionless consumer purchasing while ensuring strong authentication
- Scope may include the implementation of run-time risk calculation, web analytics, and multifactor authentication mechanisms during e-commerce transactions for a known consumer of a laboratory simulated retailer website.

# MFA EXAMPLE SCENARIO ONE

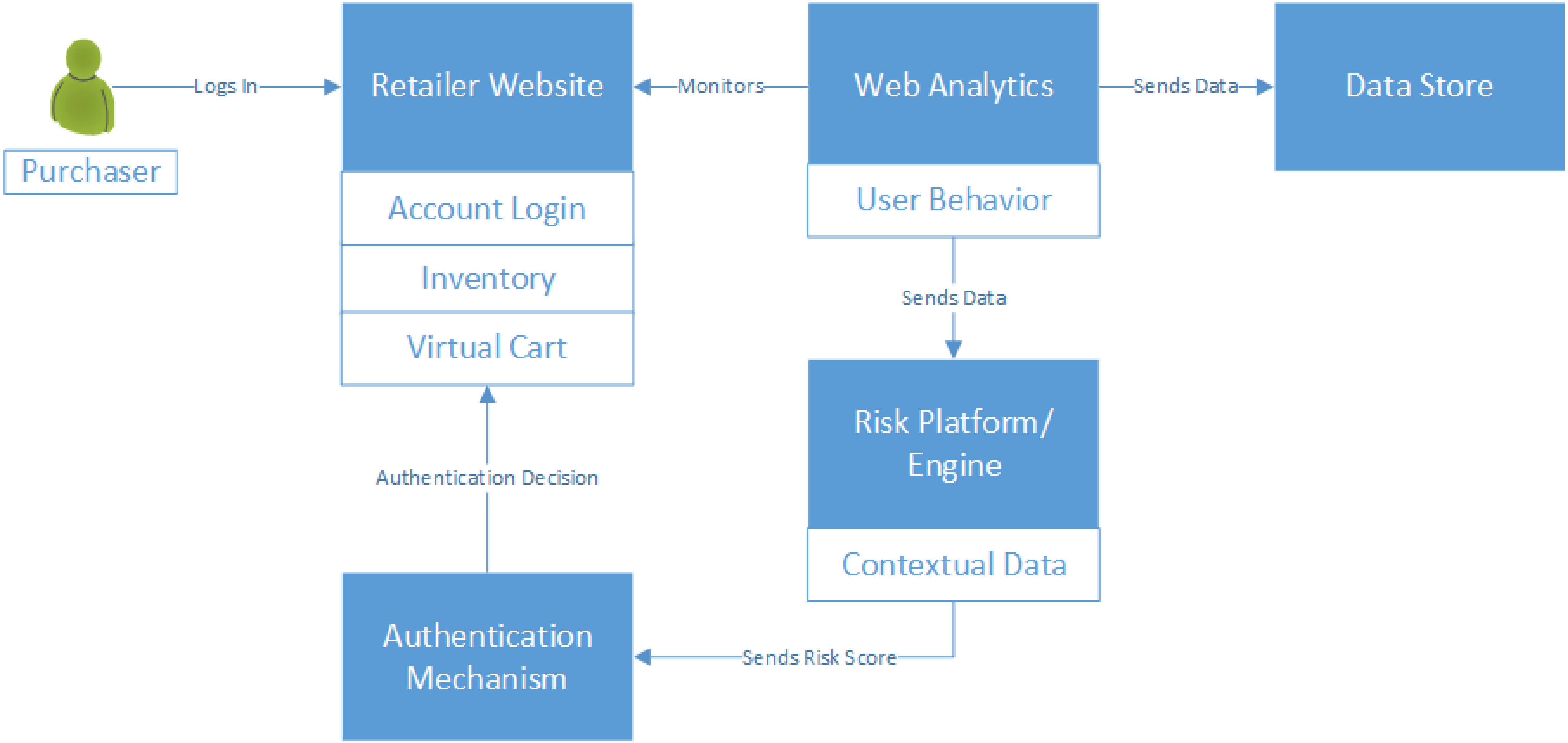
## Scenario: Repeat Customer, New Context

- While on travel for business across the country from her residence, a repeat customer of an online retailer remembers that this day would be the deadline to buy a gift online for a friend’s birthday. She opens the laptop she usually uses for work and navigates to the retailer’s website. The customer inputs a username and password to enter the site and browses several categories of expensive luxury items that she usually does not browse. After some time browsing, the customer finds a product to purchase as a gift and puts it in her virtual shopping cart. She then follows the prompts to choose shipping and stored payment methods.

- After entering these choices, the user is prompted with a message stating that, due to a security mechanism, the retailer requests she enter a multifactor authentication ID (either pre-distributed or dynamically sent via phone or email to known phone numbers or email address) before completing the transaction. The user inputs the token code received and completes the transaction.

- In the background, automated risk and web analytics on the retailer’s system are comparing this known user’s current behavior and the context of her website access to stored data. Because the user’s device, behavior, IP address, geolocation, and shopping choices do not align sufficiently per the retailer’s risk threshold and poses a relatively high fraud risk, the user is prompted for additional authentication.

# MFA HIGH-LEVEL ARCHITECTURE



# MFA EXAMPLE SCENARIO TWO

## Scenario: Fraud Perpetrator

- After illegally receiving the credentials of a legitimate, repeat customer (RC) for an online retailer, a fraud perpetrator (FP) in another country from the repeat customer navigates to the retailer's website with the intention of committing e-commerce fraud and receiving goods paid for by the RC . The FP does not browse but goes straight to an expensive electronic item, adds the item to his shopping cart, and begins the checkout process.
- During checkout the FP chooses stored payment information, but edits the shipping address to one not previously associated with the RC. After entering these choices, the malicious actor is prompted with a message requesting that he enter a multifactor authentication token ID (either pre-distributed or dynamically sent via phone or email to known numbers and addresses) as an additional step before completing the transaction. The malicious actor attempts to spoof the ID a number of times before another message appears indicating that the transaction has been terminated and the account has been locked.
- In the background, automated risk and web analytics on the retailer's system are comparing this known user's current behavior and the context of his website access to stored data. Because the user's device, behavior, IP address, geolocation, and shopping choices do not align sufficiently per the retailer's risk threshold and poses a relatively high fraud risk, the user is prompted for additional authentication. Because the retailer has implemented a limit to authentication attempts, after a few attempts the user account is locked until the retailer's fraud detection team can contact the account owner.

# MFA EXAMPLE SCENARIO THREE

## Scenario: Repeat Customer, Repeated Context

- While getting her child ready for bed a repeat customer of an online retail customer finds the supply of disposable diapers is low. The customer logs into the online retailer's website to order disposable diapers.
- She authenticates with a user ID and password. She finds the diapers in the favorites section. In seconds she places the same order for diapers that she has placed in the past.
- The online retailer grades this purchase as low risk because of the nature of the product, a known IP address associated with the customer, geolocation, and past patterns of purchases within the website.
- The customer is not prompted for any additional authentication.

# Project Requirements and Components – Questions to Consider

- Functional:
  - What will the desired architecture do? Which types of MFA should be included, what kind of online transactions will be accounted for?
- Technical:
  - Which technical components, hardware and software, would need to be included in order to implement the desired architecture?
- Interfaces:
  - How do each of the architectural components interface with each other and other relevant systems used in the online retail transaction ecosystem? How is data transmitted, and how do the components work together?
- Standards & compliance:
  - What compliance standards would relate to the desired architecture, and how would that influence how we configure or utilize a given component in the architecture?

## Proposed Components

- Online/e-commerce shopping cart and payment system (in-house or outsourced)
- Multifactor authentication mechanisms
- Risk calculation platform/engine
- Web analytics engine
- Logging of risk calculation and web analytics data
- Data storage for risk calculation and web analytics data

## Proposed Requirements

- Authentication mechanisms that meet business security and regulatory requirements
- Automated web analytics including monitoring of user behavior and contextual details
- Automated logging of web analytics and risk calculation data
- Automated data storage of web analytics and risk calculation data
- Ability to establish and enforce risk decisions including performing risk calculations
- Automated alerting of suspected fraudulent activity
- Ease of use for the consumer, no substantial increase in friction during the e-commerce transaction

# SECURING NON-CREDIT CARD, SENSITIVE CONSUMER DATA

- Growing evidence that PII is worth more on the black market than credit card numbers
- Implementation of EMV in the U.S. will likely shift fraud away from the use of counterfeit credit cards to the use of real credit cards obtained by using fake or stolen identities
- Gap to be filled in terms of understanding the risks and implementing security controls to mitigate those risks concerning non-payment PII.
- The scope should include the implementation of data masking and tokenization mechanisms for non-credit card, sensitive consumer data during commercial payment transactions both via point-of-sale (POS) and e-commerce transactions, along with fine grained attribute based access control (ABAC) for users both inside and outside an organization. A layered approach to data security including point-to-point encryption (P2PE) is generally advisable.

## Scenario : Access to sensitive data inside an organization

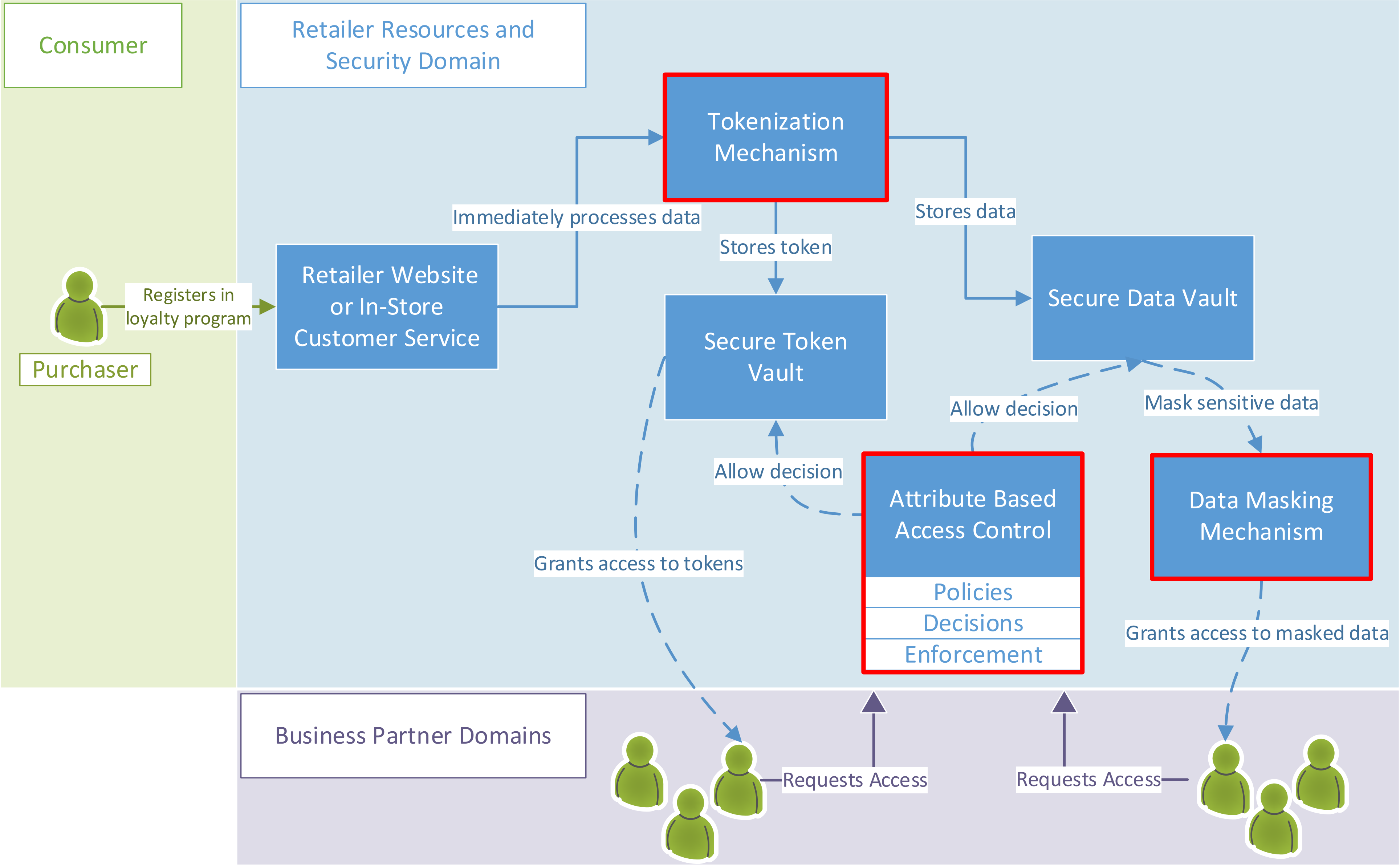
- A new customer signing up for the loyalty program of a brick-and-mortar retailer that also has an e-commerce website.
- At the Customer Service desk, the user is asked to enter the following data in order to register: name, address, email address, phone number, and date of birth.
- Receives a physical loyalty card that provides benefits including discounts both in-store and online.
- Shops in the store during the day, and then logs into the website in the evening to purchase a few more items.
- The retailer has tokenized the cardholder data as required by PCI DSS standards during the payment transaction,
- Also tokenized and data masked the non-credit card sensitive PII gathered during account registration and during the shopping trip online. The tokens are secured but accessible to parties with need-to-know access rights, while the actual raw data is stored in a highly secure data store.
- Subsequent access requests from within the retailer’s organization for the tokens or actual data are evaluated according to access control policies that correlate to the organization’s business rules and relevant standards and regulations.
- In some cases, access to the non-credit card, sensitive data  may be granted, but in many cases the token itself can be used in place of the actual data, such as internal business functions including returns, sales reports, marketing analysis, and recurring payments.
- Employees in sales, marketing, and order management and fulfillment departments are all granted access to the tokens when there is a verified need-to-know access request, but not the actual data. Customer service employees are granted access to the actual data when there is a verified need-to-know request, but with other sensitive data masked.

# SECURING DATA EXAMPLE SCENARIO TWO

## Scenario: Access to sensitive data outside an organization

- Retailer outsources its marketing analysis to a consulting company and its order fulfillment to a fulfillment house, both of whom frequently need access to some consumer data.
- All cardholder and non-cardholder, sensitive PII data are tokenized and the actual data is stored in a highly secure data store.
- A marketing analyst outside the organization has been assigned a project related to long-standing customers and shopping patterns over time.
- The analyst requests access to the purchasing habits data of the retailer’s long -standing customers.
- Instead of access to actual or masked data, the analyst is granted access to the tokens, which can still be used for the project at hand.
- When a retailer receives an online order, a fulfillment request is sent over as a token to the fulfillment house. The fulfillment house must use the token to access the real data in order to access the customer’s shipping address and ship the order.

# SECURING DATA HIGH-LEVEL ARCHITECTURE



# Project Requirements and Components – Questions to Consider

- Functional:
  - What will the desired architecture do?
- Technical:
  - Which technical components, hardware and software, would need to be included in order to implement the desired architecture?
- Interfaces:
  - How do each of the architectural components interface with each other and other relevant systems used in the online retail transaction ecosystem? How is data transmitted, and how do the components work together?
- Standards & compliance:
  - What compliance standards would relate to the desired architecture, and how would that influence how we configure or utilize a given component in the architecture?

## Proposed Components

- Online retail website or simulated customer service portal with loyalty program registration
- Tokenization mechanism
- Secure data store for tokens
- Secure data vault for actual data
- Data masking mechanism
- Attribute Based Access Control (ABAC) platform
  - Policies
  - Decision Making
  - Decision Enforcement

## Proposed Requirements

- Data tokenization and token management
  - Token generation
  - Token mapping
  - Non-credit card, sensitive consumer data vault
  - Cryptographic key management
- Data masking
- Fine-grained Attribute Based Access Control (ABAC) for internal and external users
  - Automated logging of access requests and decisions
  - Access control policy creation
  - Determining access control decisions based on policies
  - Access control policy enforcement